

Published and Copyright (c) 1999 - 2014
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,
log on to our website at: www.atarinews.org
and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org
and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to
subscribe from.

To download A-ONE, set your browser bookmarks to one of the
following sites:

<http://people.delphiforums.com/dpj/a-one.htm>
Now available:
<http://www.atarinews.org>

Visit the Atari Advantage Forum on Delphi!
<http://forums.delphiforums.com/atari/>

=~::~~::~=

~ WHO Ebola Email Scam! ~ People Are Talking! ~ Aranyrn Gets Updated!
~ FCC Adds Cybersecurity! ~ UK Threatens Web Trolls! ~ Call of Duty Specs!
~ Upstart Social Networks ~ Raymond Leaves Ubisoft! ~ Hands On with Inbox!

~ PC Tech Support Scam! ~ Brit Grandma Blocks WiFi ~ Facebook's New Rooms!

-* New Donkey Kong Secrets Found *-
-* Apple Issues iCloud Security Warning! *-
-* China: Hard To Resume Cyber Security Talks! *-

==~==~==

->From the Editor's Keyboard
"~~~~~"

"Saying it like it is!"

Election Day is rapidly approaching for many of us in the U.S. It should be an interesting event. How many of incumbent Obama supporters will manage to survive. A lot of our local coverage has tied Obama into the election equation. We'll see how this scenario pans out, soon enough!

Ebola news is still making headlines. Of course, new case has been discovered in New York. How many more cases will show up before something "significant" is done to prevent an instance which doesn't get discovered right away? We've been "lucky" so far, but we all know that luck can't last forever!

Until next time...

==~==~==

AranyM Gets An Update

Hi all developers and users of our great TOS compatible virtual machine!

I have released a new version that received so much attention and improvements in the last half of year that I could resist to bump the major version to 1. After long 13+ years of development welcome the new, much improved version. Almost every area of code was reviewed and possibly improved, mostly by Thorsten Otto, our fresh new ARAnyM developer. And Jens Heitmann did an outstanding job on the JIT area - I wouldn't be surprised if it was fully usable now (I remember myself saying that JIT was unsupported and buggy not so long ago). Would you believe you can have a TOS computer for few dollars in your pocket thanks to Raspberry Pi?

There were also certain updates by Philipp and Andreas, for OS X host and Linux guest respectively.

The source code is available at:
<http://sourceforge.net/projects/aranyM/files/aranyM/1.0.2/> and I suppose the binary packages will appear there shortly as well. I will take care

of Debian/Ubuntu packages and I kindly ask the usual builders for OS X, *.rpm, Raspberry PI and other systems to deliver me the binary packages (made from this very source code, 1.0.2.orig.tar.gz).

Also, I would love to have a SOLID binary for MS-Windows, ideally both Cygwin and MinGW (if MinGW can build it yet?). Please you with Windows who use it for primary development go ahead and send me a good tested binary, with as many compile time options enabled as possible (NFJPEG etc).

BTW, around the version 0.9.7 somebody sent me an MSI script that could be used for building an ARAnyM installer. Maybe it would be nice to have an aranymsi package that would take care of the unpacking, installing a menu item and a desktop icon. I can send the MSI to anyone who's willing to update it for 1.0 and test it thoroughly.

One more important note: I believe we need a new AFROS, or at least update the ARAnyM driver set. I think Thorsten could provide the OpenGL libraries, ideally with some cool examples? And probably new HostFS? We need to collect the up-to-date drivers somewhere and the AFROS was a good place for it.

Thank you and enjoy this new major version of ARAnyM!

Petr

2014/10/17 - version 1.0.2 released
=====

Just a quick bugfix release:

- o SDL NF CDRom is included in the build correctly
- o JIT is supported on kfreebsd-i386 (alternate kernel for Debian OS)
- o fixed errors and warnings that prevented build on Debian

2014/10/15 - version 1.0.0 released
=====

Major highlights of this release:

- o JIT CPU compiler now supports also ARM platforms driven by Linux
- o JIT CPU compiler fixes memory management and adds some instructions
- o massive NatFeat HostFS fixes and improvements (symlinks and more)
- o NatFeat CD-ROM for Win32 and SDL
- o NatFeat OSMesa support improved (OpenGL 4.4 / Mesa 10.1.4)
osmesa.ldg can replace tinygl.ldg now
- o seamless mouse integration and keyboard input improved
- o NVRAM: many country codes added (from current FreeMiNT)
- o libSDL2 is supported now (along with libSDL 1.2.x)
- o Cygwin, MinGW, Mac OS X, CentOS and Debian build fixes

Countless bug fixes and many other under-the-hood improvements are included as well. This release crowns more than 13 years of continuous development by many dedicated programmers (listed in the AUTHORS file). Thank you all!

$$= \sim = \sim = \sim =$$

```
->In This Week's Gaming Section - Assassin's Creed, Splinter Cell Producer Jade  
Raymond Leaves Ubisoft!  
    " " " " " " " " " " " " " " " " " " " " " " " " " " " " " " " " " " " "  
Call of Duty: Advanced Warfare PC Minimum Req  
uirements Revealed!  
  
    33 Years Later, New Donkey Kong Secrets Are B  
eing Found
```

$$= \sim = \sim = \sim =$$

```
->A-ONE's Game Console Industry News    -   The Latest Gaming News!
      " " " " " " " " " " " " " " " " " "
```

Assassin's Creed, Splinter Cell Producer Jade Raymond Leaves Ubisoft

Veteran Ubisoft producer Jade Raymond--who worked on franchises such as Assassin's Creed, Watch Dogs, and Splinter Cell - has left the French publisher after ten years, it was announced today. Most recently, she served as managing director of Ubisoft Toronto.

"Today, Ubisoft announced that after 10 years of collaboration, the company and Jade Raymond have agreed to pursue future opportunities separately," Ubisoft said in a statement.

Raymond will be replaced by Alexandre Parizeau, a founding member of Ubisoft Toronto, as managing director of the studio.

"I've spent 10 extraordinary years at Ubisoft, and I am proud to have been part of many of the best teams in the industry making truly remarkable games," Raymond said. "This is one of the hardest decisions of my career, but the Toronto studio is strong and on a solid path. I'm confident that now is a good time for me to transition leadership of the studio to Alex and to pursue my other ambitions and new opportunities."

"Stay tuned for more on what's next for me, but for now, I'd like to thank Ubisoft for its partnership through the years, and I wish them the very best in all their next endeavors," she added.

Raymond served as producer on the original Assassin's Creed, and worked as an executive producer on Assassin's Creed II. Other credits include Watch

Dogs and Splinter Cell: Blacklist. She has served as Ubisoft Toronto's managing director since 2009.

Raymond will officially depart Ubisoft Toronto on October 29, at which time Parizeau will become managing director. Parizeau is a 15-year veteran of the video game industry, and served as senior producer on Splinter Cell: Blacklist and producer on Splinter Cell Conviction and Rainbow Six Vegas.

Parizeau will report directly to Ubisoft Montreal and Toronto CEO Yannis Mallat.

"On behalf of Ubisoft, I'd like to thank Jade for her leadership and many contributions over the years, and wish her all the best in her next adventures," Mallat said. "The Toronto studio is a key part of the Ubisoft global network, and Alex has been at the heart of the studio's growth over the years. He was the obvious choice to lead this talented group of people as they continue to develop amazing games."

Call of Duty: Advanced Warfare PC Minimum Requirements Revealed

By way of the Steam product page for Sledgehammer Games' upcoming shooter, *Call of Duty: Advanced Warfare*, we now know the game's minimum PC system requirements.

OS: Windows 7 64-Bit / Windows 8 64-Bit / Windows 8.1 64-Bit

Processor: Intel Core™ i3-530 @ 2.93 GHz / AMD Phenom™ II X4 810 @ 2.80 GHz or better

Memory: 6 GB RAM

Graphics: NVIDIA GeForce GTS 450 @ 1GB / ATI Radeon HD 5870 @ 1GB or better

DirectX: Version 11

Network: Broadband Internet connection

Hard Drive: 55 GB available space

Sound Card: DirectX-compatible

Unfortunately, the recommended PC specifications for Advanced Warfare are not available. We'll have that information for you as soon as it becomes available.

Advanced Warfare launches November 4 (get it November 3 by preordering) for PC, Xbox 360, Xbox One, PlayStation 3, and PlayStation 4 - but not Wii U. Despite the game's release still being two weeks away, Activision just recently debuted the game's launch trailer.

$$= \sim = \sim = \sim =$$

```
->A-ONE Gaming Online  
      " " " " " " " " " " " " " " " "
```

- Online Users Grow! & Purr!

Despite the fact the game was first released in arcades in 1981, has been ported to hell and back and picked apart on the big screen, Nintendo's original Donkey Kong is still giving up secrets, most recently in the form of "new" music and sound effects.

A user on the Cutting Room wiki has, after digging through the original game's code, found three pieces of music and two sound effects that were never publicly accessible (though folks are now telling me at least some would appear in later games, including handheld ports).

One of the pieces of music is an alternate take on the tune that would play when you rescued Pauline.

The sound effects, meanwhile, are limited to Pauline yelling "help!", and another garbled clipping where it's unsure what exactly she's saying.

None of it is going to dramatically alter your experience with Donkey Kong. We're not talking new levels or developer commentary. I just find it fascinating that, as trivial as these files are, they lay dormant for almost as long as I've been alive before someone found them.

You can listen to all the tunes and effects over on the wiki (via slashdot).

=~::~~::~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

World Health Organization Ebola Email Scam

If you receive an email from the World Health Organization offering information about the Ebola virus, don't open it. The email appears to be legit, but it is only a phishing scam attempting to gain access to your computer.

Trustwave's Spider Labs published the information stated in an email, The information and prevention listed in the attached file will help you, and those around you stay safe. There is an outbreak of Ebola and other diseases around that you know nothing about. Download the World Health Organization file for more information on how to stay safe from Ebola and other preventable diseases. We care.

Clicking on the attachment will install Dark Comet Remote Access Trojan on your computer. The program can run on your computer and not be detected by antivirus software. When the program has been installed, hackers will have full access to your computer. Installation of the malware will give the hackers all logging keys pressed and passwords. The hackers will be able to upload any files on your computer and download files. The scariest part of this all is the hackers can control your webcam, by turning it on and off, including your microphone.

Everything in your environment could be seen and heard by the hackers.

It is very ordinary for hackers to use headline news stories to send out phishing emails. The United States Computer Readiness Team stated you should be suspicious of unsolicited emails and emails from unknown sources. Never click on an attachment or link that isn't recognizable.

Karl Sigler, Security Specialist at Trustwave, stated the hackers are interested in people who work in corporate environments that placing their system and the whole business network at risk.

So, don't let your curiosity get the best of you by opening any unsolicited email, it just may be a scam.

In a blog post Wednesday, Trustwave, another cybersecurity company, released a list of email subject lines that are being used in these phishing emails. Be sure to avoid emails with subject lines similar to the following:

RE: Ebola Survival Guide
What you need to know about the deadly Ebola outbreak
So Really, How Do You Get Ebola?
Ebola virus outbreak: Curing Breakthrough Revealed?
SHOCKING Health Alert: Secret Cure for Ebola?
HEALTH NEWS: Secret Cure for Ebola?
Is there ANY way to cure Ebola?
First GMO foods, now Ebola. What Obama doesn't want you to know.
Ebola, GMO, What they don't want you to know.
SHOCKING Health Alert: Ebola is spreading
EBOLA Outbreak FEMA Storing 250,000 Plastic Coffins
You won't believe what Obamacare & Ebola have in common.
Ebola Outbreak Now WORSE Than We're Being Told
Ebola & Obamacare a match made in heaven.
CDC ALERT: 1.4 Million EBOLA Victims by January?
The #1 Food Items You'll Need In An EBOLA Crisis
SHOCKING Health Alert: Secret Cure for Ebola/

China Says It's Hard To Resume Cyber Security Talks With U.S.

Resuming cyber security cooperation between China and the United States would be difficult because of "mistaken U.S. practices", China's top diplomat told U.S. Secretary of State John Kerry.

Cyber security is an irritant to bilateral ties. On Wednesday the U.S. Federal Bureau of Investigation said hackers it believed were backed by the Chinese government had launched more attacks on U.S. companies, a charge China rejected as unfounded.

In May, the United States charged five Chinese military officers with hacking American firms, prompting China to shut down a bilateral working group on cyber security.

Yang Jiechi, a state councillor overseeing foreign affairs, told Kerry in Boston the United States "should take positive action to create necessary conditions for bilateral cyber security dialogue and cooperation to resume", according to a statement seen on the Chinese Foreign Ministry

website on Sunday.

"Due to mistaken U.S. practices, it is difficult at this juncture to resume Sino-U.S. cyber security dialogue and cooperation," Yang was quoted as saying. The statement did not elaborate.

Former U.S. spy agency contractor Edward Snowden has said the U.S. National Security Agency hacked into official network infrastructure at universities in China and Hong Kong.

China, repeatedly accused by the United States of hacking, has used Snowden's allegations as ammunition to point the finger at Washington for hypocrisy.

Apple Issues Security Warning for iCloud

Apple has posted a new security warning for users of its iCloud online storage service amid reports of a concerted effort to steal passwords and other data from people who use the popular service in China.

"We're aware of intermittent organized network attacks using insecure certificates to obtain user information, and we take this very seriously," the computer-maker said in a post Tuesday on its support website. The post said Apple's own servers have not been compromised.

Apple's post did not mention China or provide any details on the attacks. But several news outlets reported Tuesday that some Chinese Internet users have begun seeing warnings that indicate they had been diverted to an unauthorized website when they attempted to sign into their iCloud accounts.

That kind of diversion, known to computer security experts as a "man in the middle" attack, could allow a third party to copy and steal the passwords that users enter when they think they are signing into Apple's service. Hackers could then use the passwords to collect other data from the users' accounts.

Chinese activists blamed the attacks on that country's government, according to news reports and the Chinese activist website GreatFire.org, which suggested the campaign was spurred by the fact that Apple recently began selling its newest iPhone models, the iPhone 6 and 6 Plus, in China. The new smartphones have software with enhanced encryption features to protect Apple users' data.

Apple, which is based in Cupertino, California, said in its post that the attacks have not affected users who sign into iCloud from their iPhones or iPads, or on Mac computers while using the latest Mac operating system and Apple's Safari browser. But the company suggested users should verify they are connecting to a legitimate iCloud server by using the security features built into Safari and other browsers such as Firefox and Google's Chrome. The browsers will show a message that warns users when they are connecting to a site that doesn't have a digital certificate verifying that it is authentic.

"If users get an invalid certificate warning in their browser while visiting www.icloud.com, they should pay attention to the warning and not proceed," Apple said in the post.

The attacks appear unrelated to an episode last month in which hackers stole nude photos from the iCloud accounts of several U.S. celebrities. In that case, Apple said its investigation concluded the hackers had obtained the users' passwords through so-called "phishing attacks" or by guessing at the answers to security questions that allowed access. The company said its servers were not breached in that case.

Court Shuts Down Alleged PC Tech Support Scam

A court has shut down a New York tech support vendor after the U.S. Federal Trade Commission accused the company of scamming computer users into paying hundreds of dollars for services they did not need.

The FTC's complaint against Pairsys, based in Albany, New York, also alleged that the company charged customers for software that was otherwise available for free.

Pairsys cold-called computer users in the U.S. and other countries, claiming to be representatives of Microsoft or Facebook, and convinced them to allow the company's workers to gain remote control over the customers' PCs as a way to diagnose computer problems, the FTC said.

Pairsys charged computer owners US\$149 to \$249 to fix nonexistent problems on their PCs, the FTC alleged.

The company also purchased deceptive online ads that led computer owners to believe they were calling technical support lines for legitimate companies, the FTC said in its complaint, filed with the U.S. District Court for the Northern District of New York in September.

Pairsys did not immediately return a message seeking comment on the FTC complaint.

Pairsys and its operators targeted seniors and other vulnerable populations, preying on their lack of computer knowledge to sell security software and programs that had no value at all, Jessica Rich, director of the FTC's Bureau of Consumer Protection, said in a statement. We look forward to getting consumers' money back in their pockets.

On Friday, the FTC announced that the court has issued a preliminary injunction against the company. The company and its officers have agreed to the injunction, which bars them from making misrepresentations to consumers about what companies they represent or whether consumers have viruses or spyware on their computer. The order also bans them from deceptive telemarketing practices, and from selling or renting their customer lists to any third party.

The injunction requires that their websites and telephone numbers must be shut down and disconnected, and their assets frozen.

After Pairsys contacted computer users through telemarketing calls or online ads, those consumers were subjected to what the FTC called a deceptive and high-pressure sales pitch from an overseas call center.

Once the Pairsys representatives had remote access to a computer, they

would tell the consumer that benign portions of the computer's OS were signs of viruses and malware, the FTC alleged. In many cases, Pairsys implied that the computer was severely compromised and had to be repaired immediately.

In its complaint, the FTC asks the court to permanently shut down the company and require the defendants to return their profits. The FTC previously brought cases against several tech support scammers in 2012 and has received settlements and judgments totaling more than \$5 million, the agency said.

FCC Adds Cybersecurity to Its Oversight

The Federal Communications Commission entered the data security business Friday with a bang, charging a record \$10 million fine against two telecommunications companies whose neglect put up to 300,000 customers at risk of identity theft.

The companies, YourTel America and TerraCom Inc., each combed the data of up to 300,000 customers to determine who was eligible for Lifeline, the FCC's low-income discount phone program. The federal assistance program has also gained the nickname Obamaphone, even though it was created in 1985 under President Ronald Reagan.

The planned fine for the two companies, which are related to each other, is the commission's first data security case and its largest privacy violation action ever.

The data the companies accessed between September 2012 and April 2013 included sensitive information like Social Security numbers, addresses, names and driver's license information. The telecoms failed to encrypt the data online, as a result, anyone could have accessed it without having to enter a password.

Although the companies discovered the security gap, they didn't alert the customers whose information had been exposed, said FCC Enforcement Bureau Chief Travis LeBlanc in a conference call with reporters on Friday. By failing to do so, LeBlanc said, both companies breached the privacy and trust of their consumers, as their privacy policies guaranteed that cybersecurity measures would protect sensitive data.

Lax security practices are the greatest factor in identity theft, the fastest growing crime in the U.S., LeBlanc said, adding that this will be the first of many data security investigations by the FCC.

Today's action serves as a warning to other carriers, he said. The Commission has sent a clear signal. We will not tolerate conduct that puts American consumers at risk of financial fraud and identity theft.

Because of data breaches at companies like Target and JPMorgan, approximately half of U.S. adults had their information stolen, but less than half of U.S. companies have taken enough precautions to protect consumer data, according to PricewaterhouseCoopers' 2014 U.S. State of Cybercrime Survey.

This move into data security by the regulator shows the Obama administration may be adding more enforcement responsibilities for

government, considering also the \$105 million fine against AT&T for unfair billing, which the Federal Trade Commission cited as part of a growing partnership on customer rights enforcement with the FCC.

Britain Threatens Internet 'Trolls' With Two Years in Jail

People found guilty of Internet "trolling" in Britain could be jailed for up to two years under government proposals outlined on Sunday, following a number of high-profile cases of abusive and threatening behaviour on Twitter.

Justice Secretary Chris Grayling told the Mail on Sunday newspaper: "This is a law to combat cruelty - and marks our determination to take a stand against a baying cyber-mob."

There has been increasing concern in Britain about the growing scourge of Internet "trolls" who post hate-filled messages on social media, often threatening their targets.

The parents of missing girl Madeleine McCann are among the most recent victims, and last month a man was jailed for 18 weeks for what prosecutors described as "a campaign of hatred" against a female lawmaker.

"These internet trolls are cowards who are poisoning our national life. No-one would permit such venom in person, so there should be no place for it on social media," Grayling said.

"That is why we are determined to quadruple the current six-month sentence."

Victims have long been calling for police and prosecutors to take online abuse more seriously and lawyers had anticipated an increase in sentences for those convicted of trolling.

"There is a public interest in having people put away for a long time," Chris Holder, of London law firm Bristows, told AFP earlier this month.

"It is putting someone in fear of their life and fear of physical harm. I think the law will develop and the sentences will go up and up."

However, some lawyers and freedom of speech campaigners have warned that criminal sanctions should be the last resort.

"Do we want to criminalise every social conduct that we find problematic?" Barbora Bukovska, a senior director at campaign group ARTICLE 19, said earlier this month.

Prosecutions can currently be brought under a number of different laws, but the Crown Prosecution Service (CPS) last year introduced guidelines to address any confusion.

It said messages sent via social media could be a criminal offence if they contain "credible threats of violence" or target an individual in a way that "may constitute harassment or stalking".

The government proposes to amend two existing laws to extend the

maximum jail term and also the time limit for prosecutions, from six months to three years.

Hands On With Inbox, Google's New Way To Experience Gmail

Google arguably reinvented email when it launched Gmail 10 years ago, but the company's never been one to stick with the status quo or shy away from a challenge. With its brand new multiplatform app called Inbox, Google is hoping - oh, yes - that it can reinvent email once again.

Inbox is a slightly confusing concept to wrap your head around. It works with Gmail as a service, but it's a completely separate interface (and as of now, at least, one that Google says will exist alongside Gmail as an option - not any sort of forced replacement). Essentially, it's a new way to think about and approach your email.

And that's where things get interesting - because the way Inbox approaches your email is, well, not very email-like. It's a clean-slate reimagining of the very way email should work and what we should gain from it.

Let's start at square one: You use Inbox either by signing into the Web app at inbox.google.com or by installing and opening the Android app or iOS app. (For now, Inbox is available only by invitation (døjà vu, anyone?); Google hasn't yet said when it'll open it up more broadly.)

After a brief introduction, you're taken to your, er, Inbox inbox - a colorful and modern-looking collection of messages and reminders, organized by both topics and dates.

There's a lot going on at once, and it's definitely going to take some getting used to. At first glance, to be completely honest, I'm a little overwhelmed.

Each cluster of items holds messages and reminders from a specific day or period of time ("Today," "Yesterday," "This month," "September," and so on). The messages are presented in what Google calls Bundles - basically an expanded version of the tab-based category system it introduced into Gmail last year. So emails determined to be promos will all be bundled together within each cluster, for instance, as will emails determined to be related to travel, purchases, or finance.

You can move messages in or out of Bundles, if you find something that doesn't belong, and you can create your own new Bundles as well - and then train Gmail to file certain types of messages into those categories. And with any Bundle, you can tap it to view all the individual messages or "sweep" the whole thing away all at once.

(Your traditional Gmail labels are still present and available, by the way; in fact, if you open up the Inbox settings, they're listed along with all the Bundles in a tab called "Labels." But there's no way to assign a message to multiple labels in this setup; a message is either in the inbox or in a single Bundle/label - and that's it. Confused yet?)

Inbox has a few other new tricks up its sleeve, like the ability to automatically pull relevant info out of messages and show it right on

the main inbox screen. That feature - known as Highlights - works with things like travel itineraries, event info, package tracking info, and photos or other files attached to an email; those types of details will be extracted and displayed right in your inbox so you can see the important stuff at a glance. Google will occasionally even look up and add pertinent details, like the phone number of a business you mentioned in a reminder or a map to a restaurant listed in a reservation confirmation.

Messages and reminders can be snoozed, which takes them out of your inbox and then causes them to reappear at whatever date and time you want. From the mobile app, you can even set a message to reappear when you arrive at a specific place, like your home or office. (Those options will be familiar to anyone who's used Boomerang, a third-party add-on that works with the regular Gmail service in a similar way.)

And speaking of snoozing, you know what term seems to have been put to bed here? Archiving. Instead of "archiving" a message in Inbox, you either snooze it, pin it - which is kind of like starring it; there's a switch at the top of the inbox that lets you view only pinned messages - or mark it as done, which takes it out of your inbox and puts it into a "Done" section (basically the equivalent of "All Mail" in the old Gmail).

Last but not least, when you go to create a new message - by clicking the floating plus sign at the bottom-right of the interface - you're now given the choice to create a new blank email, create a new email to a specific person with whom you've communicated recently, or create a new reminder.

The integration of reminders is a nice touch, though I'm still a little confused by that part of the system. Reminders I've created with Google Now on my Android phone in the past show up in Inbox, but when I create a new reminder with Google Now on my phone, it doesn't show up in Inbox. Maybe this is just an early-launch glitch, but at the moment, at least, it doesn't seem to make much sense.

As it turns out, reminders show up in the actual inbox only when their time arrives - so if you set a reminder for 5:00 p.m., it won't appear in your inbox until 5:00 p.m. You can view upcoming reminders by looking in the "Reminders" tab or the "Snoozed" tab of the Inbox app.]

So what to make of Inbox on the whole? It's hard to say. My first take is that Inbox has some really clever ideas and appealing features. The clean and modern Material Design-inspired interface is refreshing to use, for one; the native ability to snooze emails and have them reappear when needed is also quite handy. I love the prominent placement of pertinent info from messages, and the integration of reminders is a very welcome addition.

But the system in general has a lot going on, and it's all very confusing and overwhelming at first blush. Looking at Inbox, I feel slightly lost - and for a tool that's at the core of my work and personal life, that's not the kind of feeling I want to have.

I hate to say it, but Inbox reminds me a little bit of Google Wave. It's a cool concept that tries to reinvent something in such a dramatic way that it's hard to imagine many users getting on board with it. Heck, as this article has demonstrated, the concept is difficult even just to explain - which isn't usually a good sign for how easy it'll be to adopt.

Like most people, I have a love-hate relationship with my inbox. I want my email to be simplified. But when I look at Inbox right now, I don't see simplification; I see complication. And if I'm that overwhelmed by it, I can only imagine what a typical person who doesn't deal with technology all day will think.

I want to use Inbox - I really do. And I'm willing to give it a shot to see if I can get used to its unconventional ways.

The question is whether with time, this will turn into the next Gmail-like revolution - something we'll grow to love and rely on - or into the next Wave-like miscalculation, which we'll love in theory but avoid in reality.

Facebook's New App, Rooms, Wants to Make Old-School Internet Forums Cool Again

In 2011, Josh Miller left Princeton during his senior year to co-found a group blogging startup, Branch.

Branch went on to raise \$2 million from a bunch of notable investors and was advised by Twitter co-founders Evan Williams and Biz Stone. In January, it was acquired by Facebook for an estimated \$15 million.

Since then, Miller and his Branch team have been working on a stealth new app for Facebook's Creative Labs group. As part of that, he gets to have frequent meetings with Mark Zuckerberg to discuss the app's direction.

Today, Facebook is announcing what Miller is working on. The app is called Rooms, and it hopes to revive the old yet popular idea of Internet forums on mobile devices. It lets users create forums for content they're interested in. Then the administrator can invite other like-minded people to contribute to the feed with a unique QR code.

Early reports suggested that Miller's stealth project was a clone of popular anonymous apps Secret and Whisper. For Miller, it's strange to have preconceived notions about what he's building just because he's part of Facebook. Facebook has been accused of cloning other popular apps such as Snapchat and TapTalk recently.

While the app has some anonymous components, Miller's app Rooms is more like WordPress or Tumblr than a gossip-swapping site.

The reason people got excited about the Internet was because they realized, "Wow, I can find other common people to me," Miller said of the inspiration for Rooms.

For example, if you're interested in the Syracuse Orange, you can create a SU Basketball room, write a quick description, tweak the appearance of the feed, and get a discussion going.

Rooms look a lot like the layout of popular app Secret, where a large photo from a camera roll can be overlaid with text or icons. Links and videos can also be added to feeds.

Rooms are easily customizable in terms of privacy settings, color backgrounds, and even like buttons. For example, if you would rather have

forum contributors express appreciation with a beer mug emoji and the word Cheers! than a thumbs up and Like, you can set that up.

Each room has a unique QR code that can be screenshotted by an invitee. When that invitee opens Rooms, the app automatically recognizes the QR code in the user's camera roll and lets him into the forum.

Rooms isn't tied to Facebook or mobile contact lists at all. Signing up for a room requires you to create a user name of your choice, but you can have multiple user names on the app. No identifying information is collected, which is very unlike Facebook. So, much like comments sections on websites or traditional forums, fake names can be used rather than true identities.

Facebook is striving to remove all branding from the experience, the way WordPress lets blogs like TechCrunch use it without flashing its logo everywhere.

Miller's team has been working on Rooms for the past six months, most recently in London where they're spending a year collecting tech talent and collaborating with iOS guru Alan Cannistraro. Cannistraro created some of Apple's classic apps, such as iBooks.

Rooms, Miller says, wasn't a shower idea, and there was no aha! moment for it. It didn't stem from a Facebook hackathon, like Slingshot did, either.

When we joined Facebook, we were considering a few other companies, Miller says of the acquisition. Facebook was really stoked about having us work on the same problems here. What we realized at Facebook is, if you add up all the forums and message boards across the Internet, it's huge. But there are no forum apps in the top 100 mobile apps.

The product is almost too simple. There isn't a search functionality for people who are interested in participating in like-minded rooms, for example. Miller says there are a bunch of features Rooms is leaving out of launch on purpose.

We thought, Before we make this more complicated, let's see what people think, Miller says. Rooms will observe how people use the product and build out features accordingly.

Miller says Zuckerberg has been excited about Rooms, and his team has had monthly meetings with the Facebook CEO to discuss the app's progress.

When asked if he ever thinks about the fact that he was a college student three years ago, and he's now having monthly meetings with the head of Facebook, Miller laughed and said his close friends keep him grounded.

Upstart Social Networks May Fall on Their Face

Many users are sick of Facebook, but several new social networks don't yet have what it takes to beat it.

Everyone is so tired of Facebook.

Everyone has always been so tired of Facebook. In the years since Facebook grew from being a digital college yearbook to a global octopus

of connectivity, the only thing as reliable as the service's ubiquity was the avalanche of stories about how the service was on its way out.

I admit to occasionally being one of those doomsayers, but I've been impressed by Facebook's staying power. Whatever the reasons—Mark Zuckerberg's managerial prowess, the comfort of that easy blue interface, or simply the fatigue we all share at the thought of migrating to yet another new service—Facebook seems to be here to stay. Unless, of course, one of the many new challengers that have recently shown up can topple it.

For the past several weeks, I've been spending time on a couple of the new services that are rattling Facebook's cage.

First there's Ello, which made a big splash on its official premiere about a month ago and has been putting out fires ever since. Invite-only, it's a social network that promises no ads and no manipulation of user data. All of this is spelled out in Ello's manifesto. (A manifesto is always a sign that users should approach a site with not just a grain of salt but a clove of garlic and a wooden stake.)

They've clearly tapped into Facebook frustration—Ello has just raised \$5.5 million in venture capital funding. One million people are using the network, and an additional 3 million people are on the waiting list.

But.

As an early adopter, I immediately noticed some very basic problems with Ello. Let's start with the most obvious one: The search feature doesn't work.

When you log on to Ello for the first time (and the second time, and the third time, and the fourth time, if you haven't given up by then), it directs you to follow a list of graphic designer dudes whom you don't know and wouldn't necessarily want to sit next to at the artisan coffee shop.

It's impossible to find your friends, unless you manually add each one from their own pages. In order to get to their pages, you have to know their handles—are you starting to see the problem here?

There's no point in joining a social network just to follow strangers. Many of my friends have already quit.

Maybe the founders of Ello are too busy pounding drums in time to their own manifesto to care about such basic matters. Social networks are first and foremost a matter of trust, and if I can't trust the founders to let me use their network in order to be social, then I can't trust them with my personal data, either.

I also spent some time this week playing around on Tsu, which launched Oct. 14. Tsu displays ads, but it also pays back users for the content they post to the site. The more popular your content is, the more money you make, so it helps to already be a YouTube celebrity or at least a C-list Hollywood star.

If you haven't heard about Tsu yet, its \$7 million worth of venture capital funding means that you'll hear about it soon. I'm not sure, though, whether you'll want to join.

We're using a model based on royalties, and it's designed the same way that YouTube's monetization strategy was designed," said Tsu co-founder Sebastian Sobczak.

Sobczak was once a venture capitalist in San Francisco, and it shows. Early users of Tsu need to be pretty fluent in economics just to know what's going on. The site's FAQs are rife with mentions of embedded payment platforms and network adoption; the average person considering whether Tsu is the best place to brag about her engagement isn't likely to feel at home.

I asked Sobczak about that, and he insisted that it didn't matter:

Content doesn't have to be a song or a video that you make; it can be a selfie, he said. And even if you're a less social user, say you make enough over the course of the year to buy a latte. Isn't that worth it?

Maybe? I like the way Tsu works — it's easy to find people and easy to use. I like that users get a large percentage of the cash earned from their own content (Tsu takes 10 percent off the top).

But I fear that the complicated structure of the network's monetization model — and the fact that in some ways, it resembles a pyramid scheme, with greater rewards accruing to those who monetize first — will spook potential users.

People go to social networks so they can look at GIFs. Complexity is death.

I proved my own point this week. Challenged by the headaches of trying to find my friends on Ello and figure out how, exactly, I might be taken for a ride on Tsu, I closed both of the sites and logged on to Facebook. I clicked like on a couple of posts. I sniggered at a few pet photos. I posted a request and got an answer.

72-Year-Old Grandma Blocks WiFi and Mobile Signals from Her House with Special Paint

Up to this day, evidence is not clear as to whether serious health issues stem from the signals wireless devices send out. However, 72-year-old grandmother Stefanie Russell isn't taking any chances. She paid out £4,000 (\$6,412) to specialists to paint her home in anti-radiation paint, in hopes of blocking harmful WiFi and mobile phone signals, reports the Brighton Argus.

According to Russell, who resides in the UK, she suffers from electro-sensitivity, a medical impairment that causes headaches. The pain is so harsh that she can't take the bus due to the sheer number of mobile devices used onboard. I've not been diagnosed by a doctor, but my GP surgery is aware of my condition, Russell told the publication.

It makes it difficult for me to get around and see people. I don't touch the Internet or email — it's not safe.

Her solution? Four layers of anti-radiation paint, which Russell says has helped minimize the strength of wireless signals that enter her house. The painting inside and outside my house is nearly complete, said Russell. I feel much better now I'm more protected. I have a device which helps me to detect how many wireless signals are near, and I'm reassured that I will not have unwanted WiFi guests coming into my

home.

Russell s next step is to warn children in schools about the dangers of WiFi and the possible health risks that could stem from it. She believes that broadband is a safer alternative to WiFi.

=~::~~==

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.